Privacy Policy – Job Applicant

Data Controller: StrongGuard Security UK LTD, Initial Business Centre, Wilson Business Park, Manchester, M40 8WN

Data Protection Officer: Tony Bourke

As part of any recruitment process, we will collect and process personal data relating to job applicants. We are committed to being transparent about how we collect and use that data and to meeting our data protection obligations.

What information do we collect?

We collect a range of information about you. This includes:

- Your name, address and contact details, including email address and telephone number
- Details of your qualifications, skills, experience and employment / unemployment / education history
- Information about your current level of pay, including benefit entitlements
- Whether or not you have a disability for which we would need to make reasonable adjustments during the recruitment process
- Information about your entitlement to work in the UK
- Equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief

We collect this information in a variety of ways. For example, data might be contained in the application forms, CVs or resumes, obtained from your passport, or other identity documents, or collected through interviews or other forms of assessment.

We will also collect personal data about you from third parties, such as references supplied by former employers, information from employment background check providers, information from credit reference agencies and information from criminal record checks. We will seek information from third parties only once the job offer to you has been made and we will inform you that we are doing so.

Data will be stored in a range of different places, including on your application record, in HR management systems and on other IT systems (including email).

Why do we process personal data?

We need to process data to take steps, at your request, prior to entering into a contract with you. We also need to process your data in order to enter into a contract with you.

In some cases, we need to process data to ensure that we are complying with our legal obligations. For example, we are required to check a successful applicants eligibility to work in the UK before employment starts.

We have a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows us to manage the recruitment process, assess and confirm an applicants suitability for employment and decide to whom to offer a job.

We may also need to process data from job applicants to respond to and defend against legal claims.

We process health information if we need to make reasonable adjustments to the recruitment process for applicants who have a disability. This is to carry out our obligations and exercise specific rights in relation to employment.

When we process other special categories of data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is for equal opportunities monitoring purposes as permitted by the Data Protection Act 2018.

For some roles, we seek information about criminal convictions and offences. Where we seek this information, we do so because it is necessary for us to carry out our obligations and exercise specific rights in relation to employment.

For roles that require vetting to British Standards, we will seek information on employment and credit history, we do so because it is necessary for us to carry out our obligations as a security provider.

If you application is unsuccessful, we will keep your personal data on file in case there are future employment opportunities for which you may be suited. We will ask for your consent before we keep your data for this purpose, and you are free to withdraw your consent at any time by contacting dpo@strongguardsecuityuk.co.uk.

Who has access to data?

Your information will be shared internally for the purpose of the recruitment process. This includes members of the HR and recruitment team, interviewers involved in the recruitment process managers in the business department with a vacancy and IT staff if access to the data is necessary for the performance of their role.

We will not share your data with third parties unless your application for employment is successful and we make you an offer of employment. We will then share your data with former employers to obtain references for you, employment background check providers to obtain necessary background checks and the Disclosure and Barring Service to obtain necessary criminal record checks.

We will not transfer your data outside of the European Economic Area (EEA).

How do we protect data?

We take the security of your data extremely seriously. We have internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by our employees in the proper performance of their duties.

For how long do we keep data?

If your application is unsuccessful, we will hold your data on file for 12 months after the end of the relevant recruitment process. If you agree to allow us to keep your personal data on file, we will hold your data on file for a further 12 months for consideration for future employment opportunities. At the end of that period or once you withdraw your consent, your data is deleted or destroyed.

Your rights.

As a data subject, you have a number of rights. You can:

- Access and obtain a copy of your data on request
- Require us to change incorrect or incomplete data
- Require us to delete or stop processing your data, for example where the data is no longer necessary for the purpose of processing
- Object to the processing of your data where we are relying on its legitimate interests as the legal ground for processing
- Ask us to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interest override our legitimate grounds for processing data

If you would like to exercise any of these rights or make a subject access request, please contact Tony Bourke, DPO, StrongGuard Security UK LTD, Initial Business Centre, Wilson Business Park, Manchester, M40 8WN.

If you believe we have not complied with your data protection rights, you can complain to the Information Commissionaires Officer (www.ico.org.uk).

What if you do not provide personal data?

You are under no statutory or contractual obligation to provide data to us during the recruitment process. However, if you do not provide the information, we may not be able to process your application properly or at all.

If your application is successful, it will be a condition of any job offer that you provide evidence of your right to work in the UK and satisfactory references.

You are under no obligation to provide information for equal opportunities monitoring purposes and there are no consequences for your application if you choose not to provide such information.

Automated decision-making.

Some of our recruitment processes are based solely on automated decision-making.